(12) **UK Patent Application** (19) **GB** (11) **2 354 102** (13) **A**

(43) Date of A Publication 14.03.2001

(21) Application No 9921227.6

(22) Date of Filing 08.09.1999

(71) Applicant(s)
Barron McCann Limited
(Incorporated in the United Kingdom)
BeMac House, Fifth Avenue, LETCHWORTH,
Hertfordshire, SG6 2HF, United Kingdom

(72) Inventor(s)
Peter Alderson
Robert Andrew Edge

(74) Agent and/or Address for Service
Williams, Powell & Associates
4 St Paul's Churchyard, LONDON, EC4M 8AY,
United Kingdom

(51) INT CL⁷
G07F 7/10 , G06F 17/60

(52) UK CL (Edition S)
G4V VAK

(56) Documents Cited
EP 0813175 A2   WO 98/32260 A1   WO 97/50207 A1
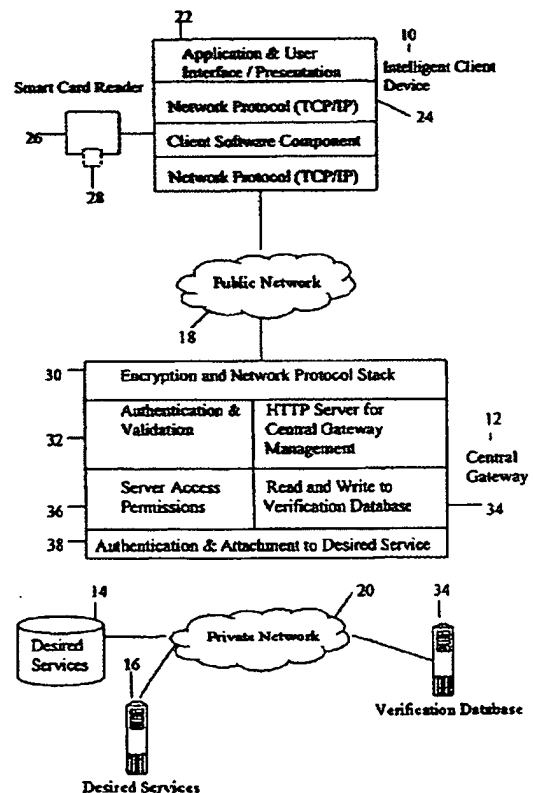WO 97/29416 A2   US 5809143 A

(58) Field of Search
UK CL (Edition R) G4V VAK , H4P PDCSA
INT CL⁷ G06F 17/60 , G07F 7/10
Online: WPI, EPODOC, JAPIO

(54) Abstract Title
System for communicating over a public network

(57) A system for communicating with a remote service over a public network 18, such as the Internet, includes a client device 10 with a memory card 28 or the like, a card reader 26 and a public network communication device such as a personal computer or television, and a processor unit, such as a central gateway 12, which is located remotely from the client device. The memory card includes user details which are transmitted by the client device to the processor unit, and may be encrypted. The card reader may activate communication with the processor unit upon insertion of the memory card, which may be a smart card or magnetic card. The processor unit may determine which of a plurality of services 14,16 a user is authorised to access. The system provides for secure communication without burdening the user with encryption or authorisation tasks.
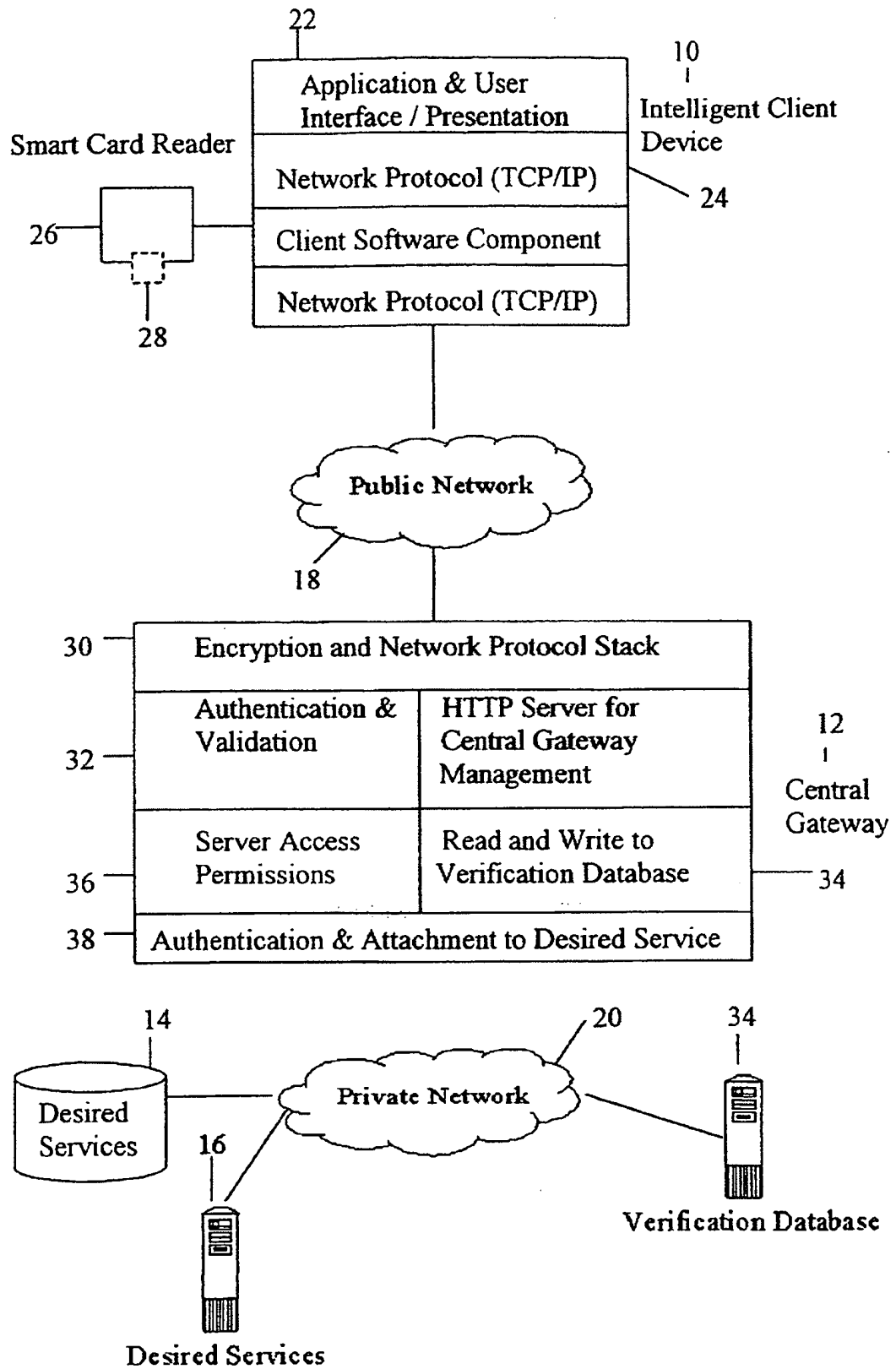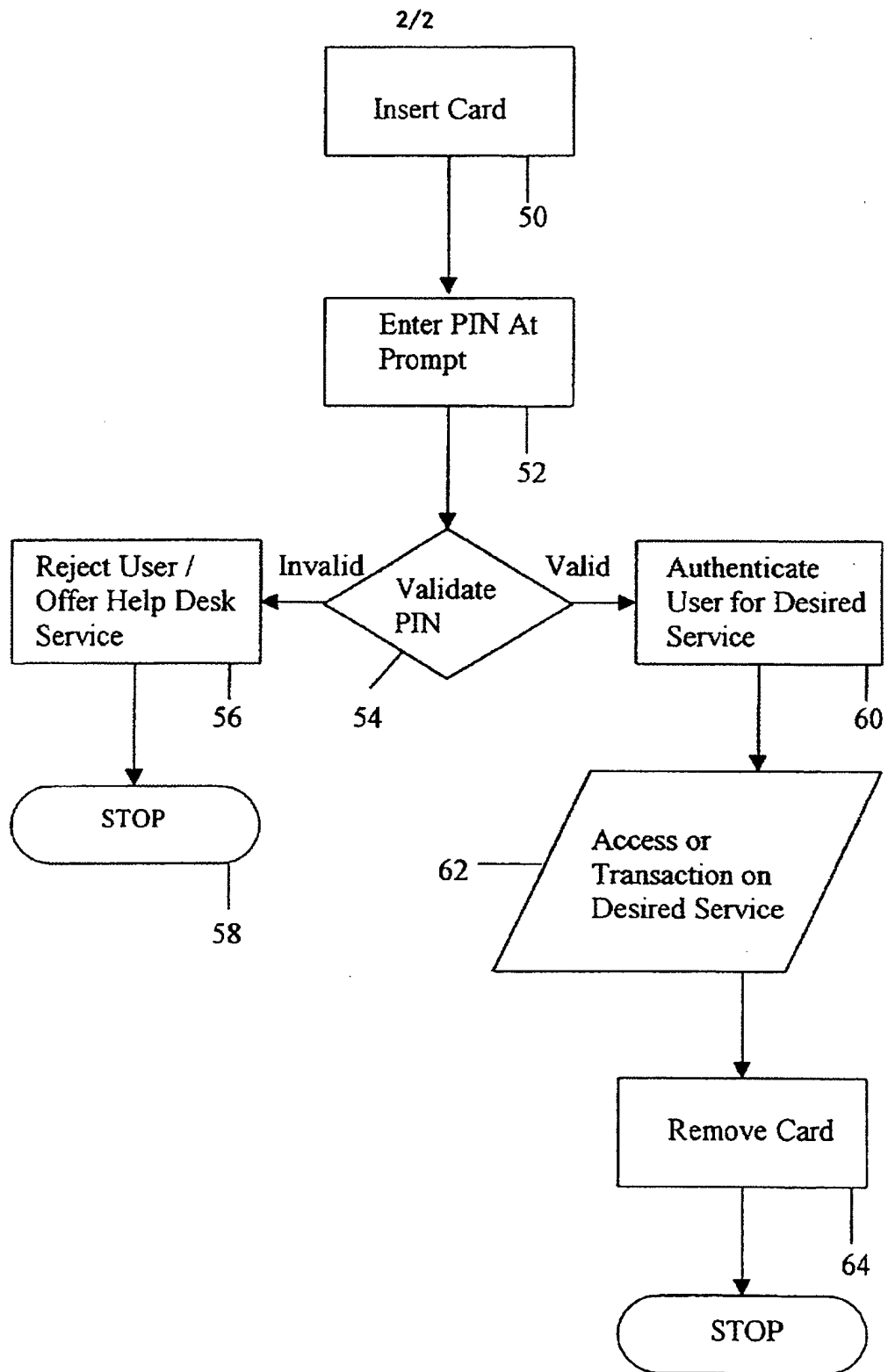
Fig 1

GB 2 354 102 A

22

Application & User
Interface / Presentation

Network Protocol (TCP/IP)

Client Software Component

Network Protocol (TCP/IP)

10

Intelligent Client
Device

24

Smart Card Reader

26

28

Public Network

18

30 — Encryption and Network Protocol Stack

32 —

Authentication & Validation	HTTP Server for Central Gateway Management
Server Access Permissions	Read and Write to Verification Database

36

34

38 — Authentication & Attachment to Desired Service

12

Central
Gateway

14

Desired
Services

16

20

Private Network

34

Verification Database

Desired Services

Fig 1

Fig 2

SECURITY SYSTEM

The present invention relates to a security system, for use for example in accessing remote services such as on the Internet.

5   With the advent of modern technology, a growing number of transactions are being carried out by the user across insecure networks. These can be, for example, transactions involving confidential data and money for payment or investment. With such transactions there are problems with security, fraud and so on. Various security systems have been devised, such as use of personal identification numbers, encryption of

10   transmissions. While these systems usually work well for the particular environment for which they have been designed, they can be a nuisance to use and can be difficult or expensive to implement for a new service provider.

Systems have also been developed for Internet use. These systems concentrate on

15   authentication of the user and then, once this has been established, provide for un-encrypted connection to the service. When particular transactions are undertaken, the service determines whether encryption is necessary, for example to secure credit card details. Other solutions require entry of credit card details for each transaction. These systems inevitably must provide a balance between security and user convenience as the

20   encryption mechanisms used cause additional work for and complication to the user.

The present invention seeks to provide an improved security system.

According to an aspect of the present invention, there is provided a security system for

25   communicating with a remote service over a public network including a user card or other memory device, a user located card or memory device reader, a user located public network communication device and a processor unit located remotely from the user located public network communication device, wherein the user card includes user details and the user located public network communication device is operable to transmit the

30   user details to the processor unit.

Advantageously, the processor unit is operable to carry out encryption between it and the user and to provide to the user a transparent path to the service. Thus, the user need not be aware of any security steps taken or any encryption system used, this being carried out by the card reader and the processor unit or central gateway.

5

The card may be any suitable device which can store user information and, preferably, encryption data. The card, can for example be a smart card, a magnetic card such as a credit/debit card or store loyalty card or any other suitable device. In addition to the card, the user may be required to input a secret identification code, such as an

10 identification number.

In the preferred embodiment, the system provides for the user to insert the card into his/her card reader and to initiate the connection to the processor unit or central gateway. Once the connection is made, the processor unit obtains the relevant data from the card

15 and upon verification by the identification code, allows the user access to the authorised service without any intermediate tasks, such as requirements to encrypt or decrypt transmitted data, to provide other user details and, where appropriate account or payment details. Thus, as with the preferred embodiment, all communications between the processor unit and the user can be encrypted, without the user necessarily being aware of

20 or involved in this encryption. The communication between the user and the processor unit can therefore be totally secure yet without user inconvenience.

Advantageously, communications between the service and the processor unit, which are preferably carried out via a secure link, need not be encrypted.

25

The splitting of the encryption from the service results in being able to provide a dedicated encryption device, the processor unit, which can therefore be designed to maximise encrypted communication efficiency. Typically, encryption of all communications from the service unit is not practicable because the service unit is not

30 designed for such a task and even if it were it would result in a loss of efficiency in providing the service itself.

In the preferred embodiment, the processor unit is also able to determine which of a plurality of services the user is authorised to access and/or the level of access such as spending limit, and to control access to the service or relevant service on this basis. It can also or alternatively undertake transactions against an account identified by the card.

An embodiment of the present invention is described below, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of an embodiment of security system coupled to a processor unit or central gateway and a service; and

Figure 2 is a flow chart of an example of validation routine for use with the system of Figure 1.

Referring to Figure 1, the embodiment of security system shown is designed for communications through the Internet or a similar public network.

The system includes an intelligence client device 10, which may be a personal computer, television, or any other suitable device which can communicate with a remote system. A processor unit, in this example a central gateway 12 is coupled between the client device 10 and one or more service units 14.

Communication between the client device 10 and the central gateway 12 is, in this embodiment, via a public network 18 such as the Internet. Communication between the central gateway 12 and the service units 14, 16 is, on the other hand, via a private network 20 which cannot be accessed by the public.

The client device 10 is provided with an application and user interface 22; which can be the usual computer devices such as monitor, keyboard and software in the case that it is a personal computer; the screen and a suitable keyboard or keypad in the case that the

device 10 is a television or any other suitable device. The device 10 could also be a portable telephone with suitable display and keypad.

The device 10 also includes suitable network protocol 24 for allowing communication to the gateway 12 through the chosen network 18 or other public transmission medium.

The device 10 also includes a card reader 26 designed for reading the card-type chosen for the system and a card 28 which is specific to that user. The card 28 could be a smart card or magnetic card of the types well known or any other portable memory device. It is envisaged that the card 28 could have other functions in addition to the security function for this system, for example it could also be a credit/debit card, store loyalty card and the like.

The card 28 has stored thereon one or more user identifiers, one or more encryption keys and the desired service information, that is details of the service to which the user wants access. His/her level of authorisation in the service and so on will be determined by the central gateway 12.

The card reader 26 is designed, in the preferred embodiment, to be able to detect the insertion of the card 28 thereinto and in response to such insertion to commence immediately communication with the gateway 12 via the client device 10.

The central gateway 12 includes an encryption and network protocol stack 30 designed to allow communication via the chosen public network 18 and to provide encryption of all communications between itself and the client device 10. It also includes an authentication and validation unit 32 for authenticating the client data from the client card 28. The authentication and validation unit 32 is coupled to a verification database 34 of the gateway 12 in which is stored the identification data of all the users registered for the services 14,16. The database 34 may be provided either within the gateway 12 or in a remote database 34' accesses through secure network 20.

The authentication and validation unit 32 is also coupled to server access permission unit 36 designed to control the type of access to the service units 14,16 in dependence upon the user's authority.

5 Also provided in the gateway 12 are a typical HTTP server for management of the gateway 12 and an authentication and attachment unit 38 for communicating with the desired services 14,16 and with any remote verification database 34'.

The central gateway 12 is designed specifically for encrypting all communications over
10 the public network 18 and for carrying out the authentication procedure.

The operation of the this embodiment will now be described with reference to Figure 2.

Insertion 50 of the card 28 into the card reader 26 prompts the card reader 26 to
15 commence automatically the connection to the gateway 12. For this purpose, card reader 26 activates a software component in the device 10 to establish a communication link with the gateway 12 on the basis of information stored on the card 28 about the location on the Internet and access details of the gateway 12.

20 When a connection with the gateway 12 is established, the gateway 12 requests the user's personal identification code which is then inputted 52 at a suitable prompt on the user interface 22.

Validation 54 of the user's details and identification code is carried out either internally
25 of the gateway 12, by the units 32 and 34, or externally at the verification database 34'.

If the gateway 12 determines 54 that the user's identification code is invalid, the user is rejected 56 and the connection is cut 58. On the other hand, if it is determined 54 the user's identification code is valid, the gateway 12 determines 60 the desired service 14,
30 16 and level of service to be provided and connects 62 to the desired service unit 14, 16.

During the connection to the desired service 14, 16, all data transfers between the gateway 12 and user device 10 are encrypted on the basis of the encryption keys on the user's card 28 and within verification database 34, while all data transfers between the gateway 12 and the service units 14, 16 through the private network 20 are not encrypted

5   for ease of access and for increased efficiency. In practice, the user will not be aware of the encryption between him/her and the gateway 12 as this will be carried out as a background task. Moreover, the user will not need to re-confirm his/her identity or financial details as these will be provided by the card 28 or gateway 12.

10   The gateway 12, in some embodiments, records the activities of the client, such as transaction details, either within the gateway 12 or in a remote memory accessed via a private network.

Disconnection from the services 14, 16 is, in this embodiment, effected simply by
15   removing 64 the card 28 from the card reader 26.

Thus, connection is made by a simple two step process of inserting the card 28 into the reader 26 and entering the user identification code and disconnection is effected by removing the card 28 from the card reader 26. The user is not involved in any other
20   authentication or encryption process and need not re-enter personal details.

This system can be used for any remote service, including business to consumer (in which case the card could be designed also to function as a store or credit card), business to business (for example for transactions on account) and for internal networking (where
25   the activity of staff, for example, needs to be secured).

It will be apparent from the above that the system can provide simple but absolutely secure access to a remote service. Moreover, by identifying the user to the desired service, user access can be customised. By removing the need for entry of account
30   details, transactions into the desired service become quicker and less risky for the user's perspective.

Performance of the services can also be enhanced by carrying out the encryption tasks within the gateway rather than in the service units.

5   In addition, the service company can establish a relationship with the user by providing the user with the card and, possibly, also with the card reader.

It will be apparent that the card 28 and card reader 26 could be configured to communicate with a plurality of separate gateways 12.

10

CLAIMS

1.   A security system for communicating with a remote service over a public network
including a user card or other memory device, a user located card or memory device
reader, a user located public network communication device and a processor unit located
remotely from the user located public network communication device, wherein the user
card includes user details and the user located public network communication device is
operable to transmit the user details to the processor unit.

2.   A security system according to claim 1, wherein the processor unit is operable to
carry out encryption between itself and the user.

3.   A security system according to claim 1 or 2, wherein the card has stored thereon
user information and, preferably, encryption data.

4.   A security system according to claim 3, wherein the card is a smart card, a
magnetic card or any other suitable device.

5.   A security system according to any preceding claim, wherein the card reader is
operable to activate communication with the remote processor means upon insertion of a
card thereinto.

6.   A security system according to any preceding claim, wherein the processor unit is
operable to encrypt substantially all communications between the user and itself.

7.   A security system according to any preceding claim, wherein the processor unit is
operable to determine which of a plurality of services a user is authenticated onto the
desired service.

8.   A security system substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.

INVESTOR IN PEOPLE

| Application No: | GB 9921227.6 | Examiner: | Michael Logan |
| Claims searched: | All | Date of search: | 20 January 2000 |

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

    UK Cl (Ed.R): G4V (VAK); H4P (PDCSA)

    Int Cl (Ed.7): G06F 17/60; G07F 7/10

Other: Online: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	EP 0813175 A2 (NCR INTERNATIONAL) whole document relevant	1-6
X	WO 98/32260 A1 (COMMONWEALTH BANK OF AUSTRALIA) see page 2 and fig 1	1-6
X	WO 97/50207 A1 (TELIA AB) see page 9, lines 1-24	1-6
X	WO 97/29416 A2 (INTEGRATED TECHNOLOGIES OF AMERICA) see especially page 7, line 5 - page 8, line 16	1-7
X	US 5809143 (HUGHES) see for example column 10, lines 35-43	1-6

16) Family number: 12389386 (JP11031130 A2) | ✉ | 🖨 | full-text | status | citations | < | > | ^ |

Title: SERVICE PROVIDING DEVICE

Priority: JP19970184866 19970710
Priority Map

Family: Family Explorer	**Publication number**	**Publication date**	**Application number**	**Application date**	**Link**
	JP11031130 A2	19990202	JP19970184866	19970710	📖

Assignee(s): FUJI XEROX CO LTD

Inventor(s): KOJIMA SHUNICHI ; KONO KENJI ; NAKAGAKI JUHEI

International class (IPC 8): G06F15/00 G09C1/00 H04L9/32 (Advanced/Invention);
G06F15/00 G09C1/00 H04L9/32 (Core/Invention)

International class (IPC 1-7): G06F15/00 G09C1/00 H04L9/32

Abstract:
Source: JP11031130A2 PROBLEM TO BE SOLVED: To
provide the utilization of service only to a user who has
a legal right, minimizing the burden on the user and a
service provider. SOLUTION: When a plug-in 38 of an
internet browser 31 is started, a verification program 15
in the plug-in 38 is started, communicates with a
program 32 for certification and performs user
authentication. A certification data generation program
A36 of the program 32 cooperates with a certification
data generation program B37 in a token 33, calculates
based on a user inherent information 16 and an access
ticket 13 and communicates with the program 15 in the
plug-in 38 based on the calculation. As the result of the
communication, the success of authentication by the
program 15 is limited to only when the three of the user
inherent information, the access ticket and enciphered
contents correctly correspond with one another.

17) Family number: 12393236 (JP11032037 A2) | ✉ | 🖨 | full-text | status | citations | < | > | ^ |

Title: CERTIFICATION DATA GENERATING DEVICE

Priority: JP19970188801 19970714
Priority Map

Family:
Family Explorer

Publication number	Publication date	Application number	Application date	Link
JP11032037 A2	19990202	JP19970188801	19970714	🖻
JP3641909 B2	20050427	JP19970188801	19970714	🖻

Assignee(s):   FUJI XEROX CO LTD

Inventor(s):   NAKAGAKI JUHEI ; SHIN YOSHIHIRO

International class (IPC 8):   G06F15/00 G06F9/06 G09C1/00 H04L9/32 (Advanced/Invention);
G06F15/00 G06F9/06 G09C1/00 H04L9/32 (Core/Invention)

International class (IPC 1-7):   G06F15/00 G06F9/06 G09C1/00 H04L9/32

Abstract:
Source: JP11032037A2 PROBLEM TO BE SOLVED: To pre-pay access qualification to purchase or rent without imposing any surplus load on a certification data generating device side. SOLUTION: A pre-paid purchase ticket T_2 is stored in an access ticket storing part 13. Next, (T_1', n_2) is inputted to a certification data-imputting part 14. A use condition judging part 15 extracts a corresponding access ticket (t_2, L_2, n_2), checks whether or not a use condition L_2 is fulfilled, and reduces frequency information V, when the use condition is fulfilled. A certification data generating and outputting part 16 calculates certification data R by using auxiliary certification decision $(t)_2$ and the use condition L_2 extracted by the use condition decision part 15 and (du) read from a user specific information storing part 11, and outputs T_1. A user performs access to a program in a purchase state or a rent state by using the T_1.
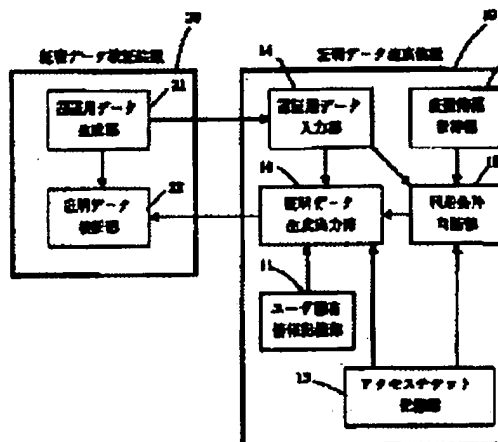
12) Family number: 13081077 (JP11205306 A2) | ☒ | 🖶 | full-text | status | citations | < | > | ^ |

Title: AUTHENTICATION SYSTEM AND AUTHENTICATION METHOD

Priority: JP19980006267 19980116
Priority Map

Family: Family Explorer	Publication number JP11205306 A2	Publication date 19990730	Application number JP19980006267	Application date 19980116	Link 🔳

Assignee(s): FUJI XEROX CO LTD

Inventor(s): KOJIMA SHUNICHI ; KONO KENJI ; TAGUCHI MASAHIRO ; TERAO TARO

International class (IPC 8): G09C1/00 H04L9/32 (Advanced/Invention); G09C1/00 H04L9/32 (Core/Invention)

International class (IPC 1-7): G09C1/00 H04L9/32

Abstract:
Source: JP11205306A2 PROBLEM TO BE SOLVED: To provide a system and method that realize diversified services by using an access ticket generated from characteristics information not belonging to a person and information specific to the user, as for the authentification system that authenticates legality of the user. SOLUTION: The authentication device 210 sends authentication data and a ticket identifier to an authentication device 250, the authentification device 250 sends the authentication data to the authentication device 210, which calculates an authentication challenge (p) based on a ticket attribute revision request (μ) and an authentication device authentification data (χ). The authentification device 250 receives the p and the (&epsi , v) to authenticate an authentication device open key based on input data and an authentication device open key identifier (v '), to authenticate the authentification device challenge and to revise contents of a ticket attribute record (VI) depending on the ticket attribute revision request (μ). Furthermore, an authentification data generating section calculates a response (R) and the authentication device authenticates the legality of the response (R).
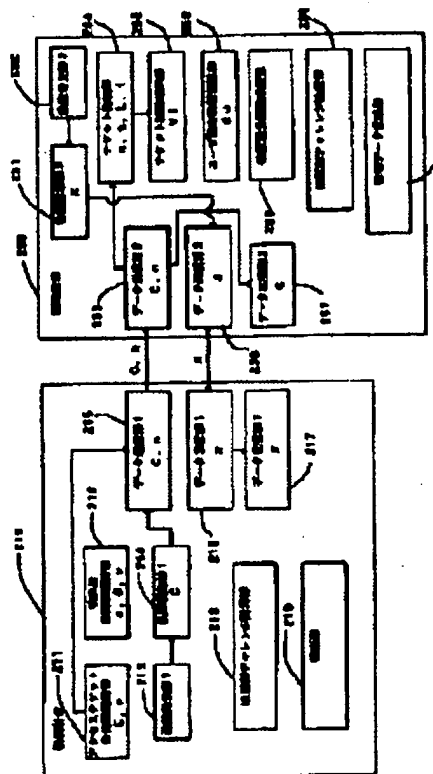
11) Family number: 13107360 (JP11215121 A2)

| ☒ | 📖 | full-text | status | citations | | > |

Title: DEVICE AND METHOD FOR AUTHENTICATION

Priority: JP19980016710 19980129
Priority Map

Family:	Publication number	Publication date	Application number	Application date	Link
Family Explorer	JP11215121 A2	19990806	JP19980016710	19980129	🖾
	JP3791169 B2	20060628	JP19980016710	19980129	🖾

Assignee(s): FUJI XEROX CO LTD

Inventor(s): KIKO KENICHIROU

International class (IPC 8): G09C1/00 H04L9/32 (Advanced/Invention); G09C1/00 H04L9/32 (Core/Invention)

International class (IPC 1-7): G09C1/00 H04L9/32

Abstract:
Source: JP11215121A2 PROBLEM TO BE SOLVED: To perform composite authentication by using the combination of different kinds of issued tickets. SOLUTION: The ticket holding section 202 of a certifying device 20 holds a ticket indicating the specific right of a user while a composite ticket holding section 206 holds a composite ticket for certifying that the user holds a plurality of other effective tickets. A certifying data generating section 203 certifies the presence of a compositely designated right by generating certifying data through executing a prescribed operation by the use of a prescribed access ticket, a composite ticket, and inherent information of the certifying device to authentication information sent from a verifying device 10.
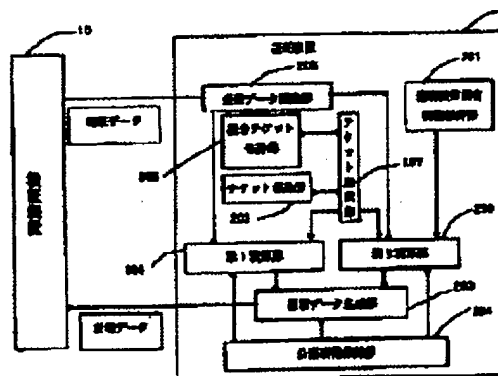
8) Family number: 14153892 (JP2000215165 A2) | ⊠ | 🖺 | full-text | status | citations | < | > | ^ |

Title:	METHOD AND DEVICE FOR INFORMATION ACCESS CONTROL AND RECORD MEDIUM RECORDII INFORMATION ACCESS CONTROL PROGRAM

Priority: JP19990017401 19990126
Priority Map

Family:	Publication number	Publication date	Application number	Application date	Link
Family Explorer	JP2000215165 A2	20000804	JP19990017401	19990126	🖻

Assignee(s): NIPPON TELEGRAPH AND TELEPHONE
(std):

Inventor(s): OHARA YASUHIRO ; OSHIMA YOSHITO

International G06F12/14 G06F15/00 G09C1/00 H04L9/32 (Advanced/Invention);
**class (IPC 8):** G06F12/14 G06F15/00 G09C1/00 H04L9/32 (Core/Invention)

International G06F12/14 G06F15/00 G06F17/60 G09C1/00 H04L9/32
class (IPC 1-7):

Abstract:
Source: JP2000215165A2 PROBLEM TO BE SOLVED: To provide the method and device for information access control which can easily change the access authority to be allowed to an accessing person in response to the change of situation of a transaction and also to provide a recording medium which records an information access control program. SOLUTION: An access ticket issuing means 1 issues the access tickets to every accessing person and these tickets prescribe the access authority to the target information for each of plural types and states. Receiving an access request from an accessing person, the means 1 reads the request and the access authority corresponding to the type and state of an inputted access ticket out of an access ticket authority information storing means 6 and decides to permit or not permit the access request based on the access authority. When a state transition request is received from the accessing person, the transition destination state is read out of a state transition information storing means 5 based on the type and state of the access ticket that is inputted together with the state transition request. Based on the transition destination state, the change of the access ticket is updated.
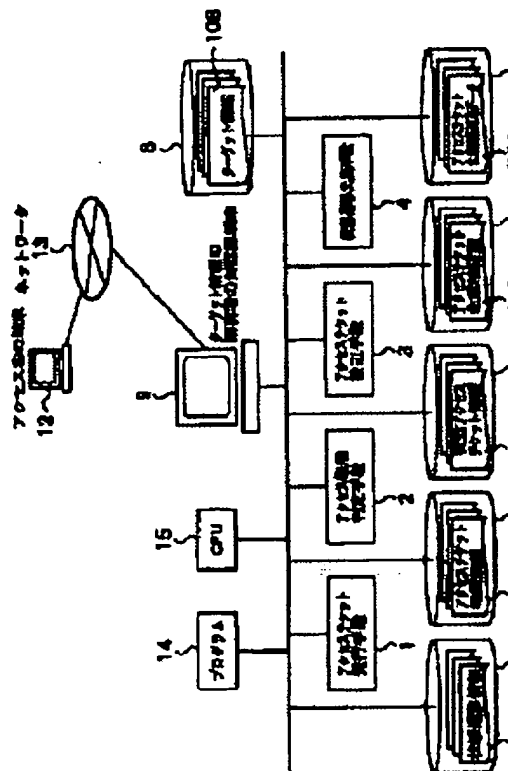
2) Family number: 33529418 (JP2005218143 A2)
extended family

|☒|🖨| ! full-
text | status | citations | < | > | ^ | ☐ | ⊕

Title: ENCRYPTION DEVICE USED IN A CONDITIONAL ACCESS SYSTEM

Priority: US19970054575P 19970801
Priority Map

Family: Family Explorer	Publication number	Publication date	Application number	Application date	Link
	JP2005218143 A2	20050811	JP20050120426	20050418	📖
	WO9907150 A1	19990211	WO1998US16145	19980731	📖🔹

Assignee(s): SCIENTIFIC ATLANTA
(std):

Assignee(s): SCIENTIFIC ATLANTA INC

Inventor(s): PALGON MICHAEL S ; PINDER HOWARD G
(std):

Designated states: AL AM AT AU AZ BA BB BE BF BG BJ BR BY CA CF CG CH CI CM CN CU CY CZ DE DK EE ES FI F GA GB GE GH GM GN GR GW HR HU ID IE IL IS IT JP KE KG KP KR KZ LC LK LR LS LT LU LV M MD MG MK ML MN MR MW MX NE NL NO NZ PL PT RO RU SD SE SG SI SK SL SN SZ TD TG TJ TR TT UA UG UZ VN YU ZW

International class (IPC 8): G09C1/00 H04L9/08 H04L9/10 H04N7/10 H04N7/16 H04N7/167 (Advanced/Invention); G09C1/00 H04L9/08 H04L9/10 H04N7/10 H04N7/16 H04N7/167 (Core/Invention)

International class (IPC 1-7): H04L9/10 H04N7/16 H04N7/167

European class: H04N7/167D H04N7/16E2

Cited documents: WO9529560, US5787172, US5592552, US5400401, US5341425, EP0752786,

Abstract:
Source: JP2005218143A2 PROBLEM TO BE SOLVED: To provide a cable television system providing conditional access to a service. SOLUTION: The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting these instances for display to system subscribers. The service instances are encrypted, by using public and/or private keys provided by service providers or central authorization agents. Keys, used by the set tops for selective decryption may also be public or private in nature, and these keys may be reassigned at different times, to provide a cable television system in which the anxiety for violation actions is minimized. COPYRIGHT: (C)2005,JPO&NCIPI<
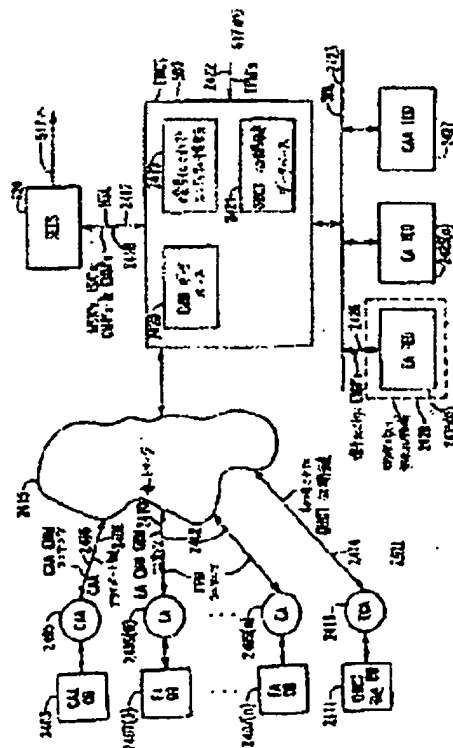
4) Family number: 33529421 (JP2005253109 A2)
extended family

Title: CONDITIONAL ACCESS SYSTEM

Priority: US19970054575P 19970801   US19980126921 19980731
Priority Map

Family:
Family Explorer

Publication number	Publication date	Application number	Application date	Link
JP2005253109 A2	20050915	JP20050120425	20050418	📧
WO9909743 A2	19990225	WO1998US16079	19980731	📧📄
WO9909743 A3	19990527	WO1998US16079	19980731	📧📄

Assignee(s): SCIENTIFIC ATLANTA
(std):

Assignee(s): SCIENTIFIC ATLANTA INC

Inventor(s): AKINS GLENDON L III ; PALGON MICHAEL S ; PINDER HOWARD G ; WASILEWSKI ANTHONY J
(std):

Inventor(s): AKINS GLENDON L

Designated states: AL AM AT AU AZ BA BB BE BF BG BJ BR BY CA CF CG CH CI CM CN CU CY CZ DE DK EE ES FI F
GA GB GE GH GM GN GR GW HR HU ID IE IL IS IT JP KE KG KP KR KZ LC LK LR LS LT LU LV M
MD MG MK ML MN MR MW MX NE NL NO NZ PL PT RO RU SD SE SG SI SK SL SN SZ TD TG TJ
TR TT UA UG UZ VN YU ZW

International class (IPC 8): H04H1/00 H04L9/08 H04N5/00 H04N7/16 H04N7/167 H04N7/173 (Advanced/Invention);
H04H1/00 H04L9/08 H04N5/00 H04N7/16 H04N7/167 H04N7/173 (Core/Invention)

International class (IPC 1-7): H04L9/08 H04N7/167

European class: H04N5/00M4 H04N7/167D H04N7/16E2

Cited documents: WO9704553, US5381481, US5029207, US4887296, US4864615, US4736422, US4613901,

Abstract:
Source: JP2005253109A2 PROBLEM TO BE SOLVED: To provide a cable television system which provides conditional access to services. SOLUTION: This cable television system includes a headend from which service "instances" or programs are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public keys and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for a selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized. COPYRIGHT: (C)2005,JPO&NCIPI<
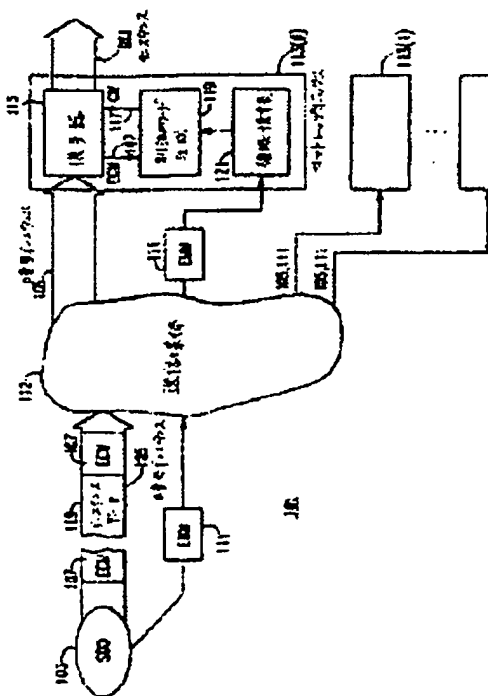
1/9/1
DIALOG(R)File 347: JAPIO
(c) 2008 JPO & JAPIO. All rights reserved.

08787202 **Image available**
CRYPTOGRAPHIC KEY SYSTEM

Pub. No.: 2006-180562 [**JP 2006180562 A**]
Published: July 06, 2006 (20060706)
Inventor: SAITO MAKOTO
        MOMIKI JUNICHI
Applicant: INTARSIA SOFTWARE LLC
Application No.: 2006-082675 [JP 200682675]
        Division of 07-346095 [JP 95346095]
Filed: March 24, 2006 (20060324)
Priority: 06-309292 [JP 94309292], JP (Japan), December 13, 1994 (19941213)

International Patent Class (v8 + Attributes)
IPC + Level Value Position Status Version Action Source Office:

    H04L-0009/08   A I F B 20060101 20060609 H JP

ABSTRACT

PROBLEM TO BE SOLVED: To provide a concrete structure for applying a cryptographic key system to a television system, a database system or an electronic commercial transaction system or the like.

SOLUTION: This system consists of a broadcasting station, a database, a receiving apparatus, a data communications apparatus and a user terminal. As a cryptographic key system, a secret-key system, a public-key system, and a digital signature system are used. The keys used in the system are either encrypted, or remain uncrypted to be supplied by broadcasting. The system is effective in preventing the unauthorized use of the database system, managing copyrights, and in pay-per-view systems and video-on-demand systems. Further, the system is effective in realizing an electronic market which uses an electronic data information system.

55) Family number: 10272458 (JP5168039 A2) | ✉ | 🖼 | full-text | status | citations | < | > | ^ |

Title: RECORDING ENCODE METHOD FOR HIGH FIDELITY TELEVISION SIGNAL

Priority: JP19910352059 19911213
Priority Map

Family: Family Explorer	**Publication number**	**Publication date**	**Application number**	**Application date**	**Link**
	JP3185806 B2	20010711	JP19910352059	19911213	🖼
	JP5168039 A2	19930702	JP19910352059	19911213	🖼

Assignee(s): SONY CORP

Inventor(s): ISHIMARU HIROYOSHI

International class (IPC 8): H04N11/22 H04N5/907 H04N9/80 H04N9/81 (Advanced/Invention); H04N11/06 H04N5/907 H04N9/80 H04N9/81 (Core/Invention)

International class (IPC 1-7): H04N11/22 H04N5/907 H04N9/80 H04N9/81

Abstract:
Source: JP5168039A2 PURPOSE: To encode a unit signal (TDM signal) for recording from a high fidelity television signal by controlling reading of plural output ports while using a serial access memory equipped with the plural output ports. CONSTITUTION: Memories 146A and 146B are serial access and two output ports are respectively provided in each memory. Then, write of input data VA and VB is controlled by memory controllers 147A and 147B, and reading of data from the respective output ports is independently controlled. Namely, TDM signals are written in memories 146A and 146B in the order of a luminance signal and a chrominance signal. In the case of reading, the same data are read from two output ports while deviating read timing, color difference signal data are extracted from the preceding output port, luminance signal data are extracted from the other output port, both data are synthesized and therefore, the required TDM signals are obtained.